Homeland Security

CIKR Cyber Information Sharing and Collaboration Program (CISCP)

In order to meet the Department of Homeland Security's (DHS) public-private cybersecurity data sharing and analytical collaboration mission, DHS has developed a Critical Infrastructure Information Sharing and Collaboration Program called CISCP.

The CISCP program mission is to improve the defensive posture of our Critical Infrastructure and Key Resource (CIKR) partner entities by, i) by sharing a view of current threats and vulnerabilities affecting both critical infrastructure and government sources among government and industry cybersecurity analysts, and by ii) aligning those analysts in collaborative engagements regarding cyber threat detection, prevention, mitigation, and response efforts to reduce risks to critical infrastructure information technology and communications networks, systems, and data. The goal of the program is an effective information sharing framework among the government, Information Sharing and Analysis Centers and related organizations, information and communications technology service providers, and their respective critical infrastructure owner/operator members and customers.

Within the CISCP program, government and industry partners contribute threat data; adding to the volume of information currently available for analysis by the DHS CISCP analytical team. Because the act of providing threat or attack data may harm competitive or other commercial interests of our industry partners, significant steps are taken to obfuscate the source of data provided as well as to protect the data provided as Protected Critical Infrastructure Information; statutorily exempting it from any release otherwise required by Freedom of Information or State Sunshine Laws, and also statutorily exempting it from regulatory use.

CISCP analysts engage in analysis of this data as well as in analytical collaboration with both government as well as industry analysts to produce accurate, relevant, timely, actionable data and analytical products. Currently, those products take the form of:

- Indicator Bulletins. Short, timely information regarding indicators of new threats and vulnerabilities based on reporting from government and CIKR provided in machine-readable-language for ease of use in threat detection and intrusion prevention capabilities.
- Analysis Bulletins. More in-depth analytic products that tie together related threat and intruder activity, describe the activity, discuss methods of detection, discuss defensive measures, and provide general remediation information.
- Alert Bulletins. Products providing an early warning of a single specific threat or vulnerability expected to have significant CIKR impact. The Alert Bulletin includes mitigation recommendations and is provided in plain text for easier ingest by the data consumer.
- Recommended Practices. Products providing, as a result of collaborative engagement regarding threats, best practice recommendations and strategies for threat detection, prevention, and mitigation.

Current processes and procedures require manual analysis and correlation. To improve the ability of CISCP to handle the anticipated volume of reporting DHS, with our critical infrastructure partners, are developing and implementing means to automate the sharing of trusted threat data; enabling more rapid abilities to ingest, correlate, and analyze data shared.